UNITED STATES DISTRICT COURT

for the

Middle District of Pennsylvania

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information associated with jjrcream69@gmail.com that is stored at premises controlled by Google LLC

Case No. 1:25-mc-00520

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC § 2252	Distribution and Possession of Child Pornography, and Attempt.

The application is based on these facts:

I, Sean McGraw, being first duly sworn, hereby depose and state as follows:

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Sean McGraw, Special Agent, FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone ~~or email~~ *(specify reliable electronic means)*.

Date: MAY 29, 2025

Judge's signature

City and state: Harrisburg, PA

Daryl F. Bloom, Chief U.S. Magistrate Judge

Printed name and title

CONTINUATION SHEETS

INTRODUCTION AND AGENT BACKGROUND

1. I make this application for a search warrant for information associated with one account – that is, jjrcream69@gmail.com (the "SUBJECT ACCOUNT") – which is stored at premises controlled by Google LLC ("PROVIDER"), an electronic communications services provider and/or remote computing services provider which is headquartered at or accepts service at 1600 Amphitheatre Parkway, Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This application is for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require PROVIDER to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B, using the procedures described in Section III of Attachment B.

2. I have been employed as a Special Agent of the Federal Bureau of Investigation ("FBI") since 2020, and I am currently assigned to

the FBI Capitol Area Resident Agency. While employed by FBI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through various trainings and through work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256(8) and used interchangeably with the term "child sexual abuse material" or "CSAM") in all forms of media, including computer media. Additionally, I have been certified in the use of various software and forensic equipment, including Cellebrite and Griffeye, for conducting digital extractions and reviews of cellular devices. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

3. The statements in this affidavit are based on my personal investigation and information provided by other law enforcement officers. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge

about this matter. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violations of Title 18, United States Code, Section 2252 (Distribution and Possession of Child Pornography, and Attempt) ("Subject Offenses"), as described in Attachment B to this affidavit will be found in the location as described in Attachment A.

JURISDICTION

4. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated.

PROBABLE CAUSE

5. On July 31, 2024, FBI was contacted by Pennsylvania State Police (PSP) Lewistown and Mifflin County Juvenile Probation concerning a minor in their supervision who had disclosed she had been in an illicit relationship with an adult male. The minor disclosed to Probation and PSP that she had been engaging in a sexual relationship with Joshua

HOCKENBERRY, DOB 7/24/1992, address (at that time) 13501 Derry Glen Court, Apartment 202, Germantown, MD 20874, for approximately nine months. Per the minor, they began a sexual relationship in approximately November 2023 after meeting at a wedding. While in a relationship, the minor disclosed that sexual images were created of the two, and that the images may be on HOCKENBERRY's cellular devices.

6. After being arrested on state corruption of minor charges by the Pennsylvania Fish and Boat Commission for being caught engaging in sexual intercourse with the minor in March 2024, HOCKENBERRY and the minor continued their sexual relationship.

7. HOCKENBERRY would travel from his home in Maryland to Lewistown, Pennsylvania, where he would pick up the minor and bring her back to Maryland for the purpose of engaging in sexual acts. The minor also reported HOCKENBERRY had bought her a cellular device. The minor's legal guardian consented to law enforcement conducting a forensic extraction of cellular devices belonging to the minor. The T MOBILE phone number 240-681-8969 was identified as a potential number belonging to HOCKENBERRY based on the nature of conversations viewed by law enforcement on the minor's cellular devices.

8. On August 6, 2024, results from a subpoena to T MOBILE indicated the subscriber of the phone number 240-681-8969 was HOCKENBERRY, with a service and billing address registered to his then-address in Germantown, MD.

9. In a review of text messages between the minor and HOCKENBERRY in July 2024, HOCKENBERRY and the minor spoke about how the minor had left items in HOCKENBERRY's vehicle:[1]

> Minor: "I think I left my red jacket in your car so if so keep it in their."
>
> HOCKENBERRY: "I'll take a look yeah you left a red jacket here."
>
> HOCKENBERRY then thanked the minor for cleaning up his apartment, and for everything she had done for him.

10. Later in the messages, HOCKENBERRY told the minor that after they were together "this past weekend," he would not see the minor for "a while." The minor then stated:

11. "The only reason why I pressure you to get me is bc you do the same thing to me just w sexual acts."

---

[1] All text messages are *sic* in these continuation sheets.

12. Later in the messages, HOCKENBERRY revealed a doorbell camera at his residence would show the minor at his residence at two o'clock in the morning. HOCKENBERRY told the minor:

> HOCKENBERRY: "I ain't saying I don't love you and I don't want to be with you [Minor's Name] I just can't keep risking it anymore we're getting closer and closer to getting caught if we didn't already caught who knows what they come back and get that doorbell camera I'm going to ask me where you're at what then. It was show me the camera footage and be like she is leaving with you at 2:00 in the morning Joshua [Hockenberry][2] where did you take her where did she go."

13. Later in the messages, HOCKENBERRY stated:

> HOCKENBERRY: "Never care about anything you never cared about the consequences of the actions you never cared about the risk and I took every time I came up to go to get you even though I warned you and told you you never cared."

14. Later in the messages, HOCKENBERRY said he and the minor were not being smart and were risking getting caught. He spoke about the directions he gave her for when he would travel to pick her up:

> HOCKENBERRY: "Just like this morning when I told you where to go where to sit swing around the block and come back around and

---

[2] The original auto-corrected: HOCKENBERRY specified in the next message that he had meant to type "Hockenberry."

you're standing right in the middle of the parking lot you don't listen to me."

15. The minor responded to HOCKENBERRY by stating:

Minor: "If you don't want to be with me than leave I mean I can't even love you right I only care about myself I'm stupid. I wanted to go home anyway but you wanted to fuck n you got that."

16. HOCKENBERRY responded to the minor's message by stating:

HOCKENBERRY: "I just said you're not going to see me for a while the cops were at my door last night that's the first time I've ever had cops beating on my door because of you being with me because I didn't trust my intuition I didn't trust my instinct and leave your ass in Pennsylvania this past weekend like I wanted to."

17. HOCKENBERRY then stated he should not have brought her to his residence in Maryland "this past weekend" and that the minor was not going to be happy until he was "locked up with nothing."

18. The minor then responded to this by stating:

Minor: "U got mad bc I didn't suck your dick and than you threaten me."

19. HOCKENBERRY then responded:

HOCKENBERRY: "That's what you want you want me to go fucking jail and you want me to risk it and keep risking it until I get busted. That's exactly what you want me to do you want me to risk

> it every single fucking week.... It's got everything to do with me being in all my legal trouble because of you and then you continuously asking me to come see you more and more and more."

20. HOCKENBERRY additionally stated, "I'm going to end up lock the fuck up for good if I continue to try and see you."

21. Later in the messages, HOCKENBERRY stated the minor had left shampoo and conditioner at his apartment, as well as took a phone charger from the residence.

22. HOCKENBERRY additionally stated:

> HOCKENBERRY: "I love you I do and I appreciate you busting your ass to clean this place up it looks so much better than it did and I'm going to miss having you here but until shit cools down I can't keep coming up and missing seeing you my luck is running out and say I'm out of town before I get caught I need to chill."

23. Later in the messages, HOCKENBERRY mentioned a sex video of the two that he was worried the minor's mother may have seen. The minor told HOCKENBERRY "Idk baby you gotta hope she didn't see it."

24. As HOCKENBERRY and the minor discussed the legality of their relationship, HOCKENBERRY stated, "Also every single text that you send is evidence. All these texts are evidence."

25. Later in the messages, HOCKENBERRY told the minor to go to the bathroom and create sexual images for him. HOCKENBERRY stated, "Come on babe its for me do it for me. Just a couple more pictures...." The minor refused to take the requested photos.

26. On August 9, 2024, the case agent found several images of HOCKENBERRY on the minor's device. These images consisted of HOCKENBERRY shirtless laying in what appeared to be a bed with the minor, who was also shirtless. These images did not meet the legal definition of CSAM.

27. HOCKENBERRY also persuaded the minor to delete evidence of their relationship. On July 26, 2024, HOCKENBERRY questioned her to see if she had deleted all evidence of contact between the two, including photographs and sex videos created by the two, prior to her phone being given to Mifflin County Probation. HOCKENBERRY reminded the minor of how he taught her to delete and reset the data storage on her cellular device. The minor stated, "Yeah I deleted everything." HOCKENBERRY then sent numerous messages stating he was going to get arrested by law enforcement because of the items on the minor's devices. HOCKENBERRY also sent her an article from stuartmillersolicitor.co.uk/ that

detailed what data law enforcement can access during a forensic review of devices.

28. After the minor provided electronic evidence to law enforcement, HOCKENBERRY sent the following threatening text messages to her:

> You think I'm joking already know where y'all live now I'm going to come up there tonight I'm going to beat your fucking face fucking in
>
> I'm going to beat your fucking face and so fucking good it's going to feel so good feeling your fucking jaws break underneath my fucking fist I swear to God and watching your nose cave the fuck in and play go everywhere I'm going to enjoy that shit so much
>
> I'm going to break your fucking nose
>
> I cannot wait to break your fucking face
>
> I swear to God I'm going to come up there and smack you fucking teeth out your head

29. HOCKENBERRY was arrested for the offenses related to this investigation in November 2024. During the arrest, HOCKENBERRY had a cellular device with him at the premise. The item was seized by law enforcement, and with the authority of a search warrant, law enforcement completed a forensic review of the device. During the review, the

case agent found multiple images of the minor victim engaging in sexual conduct with an adult male.

30. In an interview with the minor victim on April 22, 2025, they positively identified themselves and HOCKENBERRY in the images.

31. In a review of phone calls and text messages HOCKENBERRY placed to his family from February through April 2025 while he was incarcerated at Dauphin County Prison, HOCKENBERRY instructed a member of his family on how to unlock what the case agent believed to be a cellular device belonging to HOCKENBERRY not seized by law enforcement during his arrest in November 2024. HOCKENBERRY instructed the individual on how to unlock the phone, then gave specific instructions related to accessing his Google account. Once the family member confirmed the access, HOCKENBERRY instructed the family member to store the phone and to not reveal its location to anyone.

32. In a review of HOCKENBERRY's device seized during his arrest, the case agent found the Gmail address jjrcream69@gmail.com was connected to the device. The Gmail account appeared to be in use on the device from approximately August 2024 until November 2024.

33. On May 20, 2025, an administrative subpoena return indicated the subscriber to the Gmail account was HOCKENBERRY. According to the return, the account was created on August 8, 2024, with HOCKENBERRY listed as the Google Pay Contact. Additionally, the postal address registered to the account was 13501 Derry Glen Ct, Apt 202, Germantown, MD 20874, which is HOCKENBERRY's former Maryland address.

GOOGLE RECORDS

34. As noted above, the Subject appeared to regularly use the Gmail jjrcream69@gmail.com.

35. Based on my training and experience, I know that email accounts often contain evidence of crimes, to include communications with other coconspirators, evidence of preplanning and coordination, and other relevant information.

36. Therefore, there is probable cause to believe that information held by Google associated with Gmail address jjrcream69@gmail.com will contain evidence and information of HOCKENBERRY's illegal activity.

BACKGROUND CONCERNING PROVIDER'S ACCOUNTS

37. PROVIDER is the provider of the internet-based account identified by jjrcream69@gmail.com.

38. PROVIDER provides its subscribers internet-based accounts that allow them to send, receive, and store e-mails online. PROVIDER accounts are typically identified by a single username, which serves as the subscriber's default e-mail address, but which can also function as a subscriber's username for other PROVIDER services, such as instant messages and remote photo or file storage.

39. Based on my training and experience, I know that PROVIDER allows subscribers to obtain accounts by registering on PROVIDER's website. During the registration process, PROVIDER asks subscribers to create a username and password, and to provide basic personal information such as a name, an alternate e-mail address for backup purposes, a phone number, and in some cases a means of payment. PROVIDER typically does not verify subscriber names. However, PROVIDER does verify the e-mail address or phone number provided.

40. Once a subscriber has registered an account, PROVIDER provides e-mail services that typically include folders such as an "inbox" and a "sent mail" folder, as well as electronic address books or contact lists, and all of those folders are linked to the subscriber's username. PROVIDER subscribers can also use that same username or account in connection with other services provided by PROVIDER.

41. In general, user-generated content (such as e-mail) that is written using, stored on, sent from, or sent to a PROVIDER account can be permanently stored in connection with that account, unless the subscriber deletes the material. For example, if the subscriber does not delete an e-mail, the e-mail can remain on PROVIDER's servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to exist on PROVIDER's servers for a certain period of time.

42. Thus, a subscriber's PROVIDER account can be used not only for e-mail but also for other types of electronic communication, including instant messaging, photo and video sharing, voice calls, video chats, SMS text messaging, and social networking. Depending on user settings, user-generated content derived from many of these services is normally stored on PROVIDER's servers until deleted by the subscriber. Similar to e-

mails, such user-generated content can remain on PROVIDER's servers indefinitely if not deleted by the subscriber, and even after being deleted, it may continue to be available on PROVIDER's servers for a certain period of time. Furthermore, a PROVIDER subscriber can store contacts, calendar data, images, videos, notes, documents, bookmarks, web searches, browsing history, and various other types of information on PROVIDER's servers. Based on my training and experience, I know that the types of data discussed above can include records and communications that constitute evidence of criminal activity.

43. Based on my training and experience, I know that providers such as PROVIDER also collect and maintain information about their subscribers, including information about their use of PROVIDER's services. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. Providers such as PROVIDER also commonly have records of the

Internet Protocol address ("IP address") used to register the account and the IP addresses associated with other logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which devices were used to access the relevant account. Also, providers such as PROVIDER typically collect and maintain location data related to subscriber's use of PROVIDER services, including data derived from IP addresses and/or Global Positioning System ("GPS") data.

44. Based on my training and experience, I know that providers such as PROVIDER also collect information relating to the devices used to access a subscriber's account – such as laptop or desktop computers, cell phones, and tablet computers. Such devices can be identified in various ways. For example, some identifiers are assigned to a device by the manufacturer and relate to the specific machine or "hardware," some identifiers are assigned by a telephone carrier concerning a particular user account for cellular data or voice services, and some identifiers are assigned by PROVIDER to track what devices are using PROVIDER's accounts and services. Examples of these identifiers include a unique application number, hardware model, operating system version, Global

Unique Identifier ("GUID"), device serial number, mobile network information, telephone number, Media Access Control ("MAC") address, and International Mobile Equipment Identity ("IMEI"). Based on my training and experience, I know that such identifiers may constitute evidence of the crimes under investigation because they can be used (a) to find other PROVIDER accounts created or accessed by the same device and likely belonging to the same user, (b) to find other types of accounts linked to the same device and user, and (c) to determine whether a particular device recovered during the course of the investigation was used to access the PROVIDER account.

45. PROVIDER also allows its subscribers to access its various services through an application that can be installed on and accessed via cellular telephones and other mobile devices. This application is associated with the subscriber's PROVIDER account. In my training and experience, I have learned that when the user of a mobile application installs and launches the application on a device (such as a cellular telephone), the application directs the device in question to obtain a Push Token, a unique identifier that allows the provider associated with the application (such as PROVIDER) to locate the device on which the

application is installed. After the applicable push notification service (*e.g.*, Google Cloud Messaging) sends a Push Token to the device, the Token is then sent to the application, which in turn sends the Push Token to the application's server/provider. Thereafter, whenever the provider needs to send notifications to the user's device, it sends both the Push Token and the payload associated with the notification (*i.e.*, the substance of what needs to be sent by the application to the device). To ensure this process works, Push Tokens associated with a subscriber's account are stored on the provider's server(s). Accordingly, the computers of PROVIDER are likely to contain useful information that may help to identify the specific device(s) used by a particular subscriber to access the subscriber's PROVIDER account via the mobile application.

46. Based on my training and experience, I know that providers such as PROVIDER use cookies and similar technologies to track users visiting PROVIDER's webpages and using its products and services. Basically, a "cookie" is a small file containing a string of characters that a website attempts to place onto a user's computer. When that computer visits again, the website will recognize the cookie and thereby identify the same user who visited before. This sort of technology can be used to

track users across multiple websites and online services belonging to PROVIDER. More sophisticated cookie technology can be used to identify users across devices and web browsers. From training and experience, I know that cookies and similar technology used by providers such as PROVIDER may constitute evidence of the criminal activity under investigation. By linking various accounts, devices, and online activity to the same user or users, cookies and linked information can help identify who was using a PROVIDER account and determine the scope of criminal activity.

47. Based on my training and experience, I know that PROVIDER maintains records that can link different PROVIDER accounts to one another, by virtue of common identifiers, such as common e-mail addresses, common telephone numbers, common device identifiers, common computer cookies, and common names or addresses, that can show a single person, or single group of persons, used multiple PROVIDER accounts. Based on my training and experience, I also know that evidence concerning the identity of such linked accounts can be useful in identifying the person or persons who have used a particular PROVIDER account.

48. Based on my training and experience, I know that subscribers can communicate directly with PROVIDER about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Providers such as PROVIDER typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

49. In summary, based on my training and experience in this context, I believe that the computers of PROVIDER are likely to contain user-generated content such as stored electronic communications (including retrieved and unretrieved e-mail for PROVIDER subscribers), as well as PROVIDER-generated information about its subscribers and their use of PROVIDER services and other online services. In my training and experience, all of that information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. In fact, even if subscribers provide

PROVIDER with false information about their identities, that false information often nevertheless provides clues to their identities, locations, or illicit activities.

50. As explained above, information stored in connection with a PROVIDER account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element of the offense, or, alternatively, to exclude the innocent from further suspicion. From my training and experience, I know that the information stored in connection with a PROVIDER account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, e-mail communications, contact lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by PROVIDER can show how and when the account was accessed or used. For example, providers such as PROVIDER typically log the IP addresses from which users access the account along with the time and date. By determining the physical

location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the PROVIDER account access and use relating to the criminal activity under investigation. This geographic and timeline information may tend to either inculpate or exculpate the person who controlled, used, and/or created the account. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via e-mail). Finally, stored electronic data may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information in the PROVIDER account may indicate its user's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).[3]

---

[3] At times, internet services providers such as PROVIDER can and do change the details and functionality of the services they offer. While the information in this section is true and accurate to the best of my knowledge and belief, I have not specifically reviewed every detail of PROVIDER's services in connection with submitting this application for

51. Based on my training and experience, I know that evidence of who controlled, used, and/or created a PROVIDER account may be found within the user-generated content created or stored by the PROVIDER subscriber. This type of evidence includes, for example, personal correspondence, personal photographs, purchase receipts, contact information, travel itineraries, and other content that can be uniquely connected to a specific, identifiable person or group. In addition, based on my training and experience, I know that this type of user-generated content can provide crucial identification evidence, whether or not it was generated close in time to the offenses under investigation. This is true for at least two reasons. First, people that commit crimes involving electronic accounts (*e.g.*, e-mail accounts) typically try to hide their identities, and many people are more disciplined in that regard right before (and right after) committing a particular crime. Second, earlier-generated content may be quite valuable, because criminals typically improve their tradecraft over time. That is to say, criminals typically

---

a search warrant. Instead, I rely upon my training and experience, and the training and experience of others, to set forth the foregoing description for the Court.

learn how to better separate their personal activity from their criminal activity, and they typically become more disciplined about maintaining that separation, as they become more experienced. Finally, because e-mail accounts and similar PROVIDER accounts do not typically change hands on a frequent basis, identification evidence from one period can still be relevant to establishing the identity of the account user during a different, and even far removed, period of time.

AUTHORIZATION REQUEST

76. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

77. I further request that the Court direct PROVIDER to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrant will be served on PROVIDER, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

CONCLUSION

78. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence of the Subject Offenses may be located with the records and information associated with the SUBJECT ACCOUNT described in Attachment A. Therefore, I request that the Court issue the proposed search warrant to seize items described in Attachment B.

CONCLUSION

52. Based on the foregoing, I request that the Court issue the proposed search warrant.

53. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on Google. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

ATTACHMENT A
Property to be Searched

This warrant applies to information that is associated with the accounts identified by jjrcream69@gmail.com, which is stored at premises owned, maintained, controlled, or operated by Google LLC, a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California.

ATTACHMENT B

Particular Things to be Seized and Procedures to Facilitate Execution of the Warrant

I. Information to be disclosed by Google LLC ("PROVIDER") to facilitate execution of the warrant

To the extent that the information described in Attachment A is within the possession, custody, or control of PROVIDER, including any records that have been deleted but are still available to PROVIDER, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), PROVIDER is required to disclose the following information to the government corresponding to each account or identifier ("Account") listed in Attachment A:

a. For the time period August, 8,2024 – present: The contents of all communications and related transactional records for all PROVIDER services used by an Account subscriber/user (such as e-mail services, calendar services, file sharing or storage services, photo sharing or storage services, remote computing services, instant messaging or chat services, voice call services, or remote computing services, *e.g.*, Google Drive), including but not limited to incoming, outgoing, and draft e-mails,

messages, calls, chats, and other electronic communications; attachments to communications (including native files); source and destination addresses and header or routing information for each communication (including originating IP addresses of e-mails); the date, size, and length of each communication; and any user or device identifiers linked to each communication (including cookies); electronic communication services such as Google Voice (voice calls, voicemail, and SMS text messaging), Hangouts (instant messaging and video chats), Google+ (social networking), Google Groups (group discussions), Google Photos (photo sharing), and YouTube (video sharing); web browsing and search tools such as Google Search (internet searches), Web History (bookmarks and recorded browsing history), and Google Chrome (web browser); online productivity tools such as Google Calendar, Google Contacts, Google Docs (word processing), Google Keep (storing text), Google Drive (cloud storage), Google Maps (maps with driving directions and local business search) and other location services, and Language Tools (text translation); online tracking and advertising tools such as Google Analytics (tracking and reporting on website traffic) and Google

AdWords (user targeting based on search queries); Pixel Phone (services which support a Google smartphone); and Google Play (which allows users to purchase and download digital content, e.g., applications).

b. For the time period August, 8,2024 – present: The contents of all other data and related transactional records for all PROVIDER services used by an Account user (such as e-mail services, calendar services, file sharing or storage services, photo sharing or storage services, remote computing services, instant messaging or chat services, voice call services, or remote computing services, *e.g.*, Google Drive , including any information generated, modified, or stored by user(s) or PROVIDER in connection with the Account (such as contacts, calendar data, images, videos, notes, documents, bookmarks, profiles, device backups, and any other saved information);

c. For the time period August, 8,2024 – present: All PROVIDER records concerning the online search and browsing history associated with the Account or its users (such as information collected through tracking cookies);

d. For the time period August, 8,2024 – present: All records and other information concerning any document, or other computer file created, stored, revised, or accessed in connection with the Account or by an Account user, including the contents and revision history of each document or other computer file, and all records and other information about each connection made to or from such document or other computer file, including the date, time, length, and method of connection; server log records; data transfer volume; and source and destination IP addresses and port numbers;

e. All records regarding identification of the Account, including names, addresses, telephone numbers, alternative e-mail addresses provided during registration, means and source of payment (including any credit card or bank account number), records of session times and durations (including IP addresses, cookies, device information, and other identifiers linked to those sessions), records of account registration (including the IP address, cookies, device information, and other identifiers linked to account registration), length of service and types of

services utilized, account status, methods of connecting, and server log files;

f. All records pertaining to devices associated with the Account and software used to create and access the Account, including device serial numbers, instrument numbers, model types/numbers, International Mobile Equipment Identities ("IMEI"), Mobile Equipment Identifiers ("MEID"), Global Unique Identifiers ("GUID"), Electronic Serial Numbers ("ESN"), Android Device IDs, phone numbers, Media Access Control ("MAC") addresses, operating system information, browser information, mobile network information, information regarding cookies and similar technologies, and any other unique identifiers that would assist in identifying any such device(s), including unique application numbers and push notification tokens associated with the Account.

g. Basic subscriber records and login history (including, as described in 18 U.S.C. § 2703(c)(2), names, addresses, records of session times and durations, length of service and types of service utilized, instrument numbers or other subscriber numbers or identities, and

payment information) concerning any PROVIDER account (including both current and historical accounts) ever linked to the Account by a common e-mail address (such as a common recovery e-mail address), or a common telephone number, means of payment (*e.g.*, credit card number), registration or login IP addresses (during one-week period), registration or login cookies or similar technologies, or any other unique device or user identifier;

h. All information held by PROVIDER related to the location and location history of the user of the Account, including geographic locations associated with the Account (including those collected for non-PROVIDER based applications), IP addresses, Global Positioning System ("GPS") information, and information pertaining to nearby devices, Wi-Fi access points, and cell towers;

i. All IP addresses and associated port information

j. For the time period August 8, 2024 – present: All records of communications between PROVIDER and any person regarding the Account, including contacts with support services and records of actions taken;

k. Information about any complaint, alert, or other indication of malware, fraud, or terms of service violation related to the Account or associated user(s), including any memoranda, correspondence, investigation files, or records of meetings or discussions about the Account or associated user(s) (but not including confidential communications with legal counsel);

Within 14 days of the issuance of this warrant, PROVIDER shall deliver the information set forth above via United States mail, courier, or e-mail to the following:

Sean McGraw, Special Agent, FBI
stmcgraw@FBI.GOV
3501 Concord Road, Suite 300, York PA 17402

This warrant authorizes a review of records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and

agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review

Government Procedures for Warrant Execution

The United States government will conduct a search of the information produced by PROVIDER and determine which information is within the scope of the information to be seized specified in Section II. That information that is within the scope of Section II may be copied and retained by the United States.

Law enforcement personnel will then seal any information from PROVIDER that does not fall within the scope of Section II and will not further review the information absent an order of the Court. Such sealed information may include retaining a digital copy of all information received pursuant to the warrant to be used for authentication at trial, as needed.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents,

attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.